様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ３ 日現在

機関番号：３４５０４
研究種目：基盤研究(C)（一般）
研究期間：2012～2015
課題番号：２４５６０４８６

研究課題名（和文）物理層セキュリティの実用に向けた理論と符号化の構築

研究課題名（英文）Study on theory and coding schemes for physical layer security

研究代表者
井坂　元彦（Isaka, Motohiko）

関西学院大学・理工学部・教授

研究者番号：５０３５１７３９

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：ディジタル通信における雑音を積極的に利用して通信の安全性を実現する物理層セキュリティを検討した．特に秘密鍵共有プロトコルを対象として，雑音通信路の出力を基に通信を行う二者が共通のビット列を生成する手順に関する性能解析を行った．この状況は，復号器に補助情報が与えられた順序つき確率変数列に対する情報源符号化として定式化でき，確率変数列の統計的性質を踏まえた誤り確率の理論的解析を行った．得られた結果により，誤り率特性を精度良く予測することが可能となった．また，この手順に関わる線形符号の構成，および量子化の手法についても検討を行った．

研究成果の概要（英文）：We studied aspects of physical layer security in which noise on communication channels is exploited as resource for secrecy. Our focus is on secret key agreement with public discussion, and we analyzed the probability that two parties fail to agree on a common information. This problem is formulated as coding for ordered random variables with side information at the decoder, and statistical property of the associated signal sequence needs to be considered. Our analyses successfully predict the performance of the coding scheme. Construction of linear codes and quantization used in this protocol are also investigated.

研究分野：情報理論・符号理論とその応用

キーワード：物理層セキュリティ　符号化　補助情報　誤り確率

１．研究開始当初の背景

通信の守秘を目的として使用される暗号技術は，その安全性を計算量的な仮定に依拠するものが実用化されている．しかしながら，この仮定の妥当性は数学的に証明されていないため，将来にわたって安全性が担保される保証はない．この事実を背景に，攻撃者の計算能力に制限を設けない状況においても安全性が確保される暗号方式の必要性が認識されている．

このような情報理論的安全性を実現するためには，計算量以外の現実的な仮定を利用する必要がある．ひとつの手法として，ディジタル通信における通信路で発生する雑音のランダム性を積極的に利用する物理層セキュリティが挙げられる．特に，第三者が得る情報量が所望の値以下であるような秘密情報を，通信を行う二者間で共有するための方法は，本分野における重要な問題となっている．これは，情報理論的な立場から興味深い問題であるため，特に最近 10 年ほどの間に様々な設定の下で研究が行われてきた．さらに，学術的な意義に加えて，通信システムにおいて普遍的に存在する物理現象を利用することで簡易に通信の守秘を達成できることから，実用的な意義も大きい話題である．

２．研究の目的

本研究は，物理層セキュリティのひとつの実現形態である「秘密鍵共有プロトコル」を検討対象とする．すなわち，２人のプレイヤー，アリスとボブが第３者の存在の下で秘密鍵の生成を行うことを目指す．なお，二者間での守秘通信は，このプロトコルで共有された秘密鍵を使い捨ての暗号鍵として利用することで行われる．

このプロトコルは以下の手順からなる

- アリスは信号列を送信し，ボブは雑音通信路の出力として信号列を受信する
- 両者は，得られた信号列に対して誤り訂正符号の手法を適用することで共通のビット列を生成する
- 共有されたビット列に対してある種の圧縮を行うことで，秘密鍵を生成する

なお，上記の設定では両プレイヤーの間で雑音通信路に加えて，メッセージ認証がされた公開通信路が利用可能であることを仮定する．さらに，第三者はボブと同様，雑音通信路の出力として信号列を受信しており，また公開通信路における通信内容を把握できる立場にあるとする．

この手法に対して，情報理論分野の中でも情報量的な側面を扱うシャノン理論的な観点から，安全に共有可能な秘密鍵の情報量に関する解析が行われている．一方，無線通信で見られる通信路，特に送信者・受信者間に存在するマルチパスフェージングの特性が双方向で同一である性質を利用した実験的な検討または計算機シミュレーションによる研究が行われている．

このように，情報量的観点と実践的立場からの研究は盛んに行われているが，秘密鍵共有プロトコルの具現化に向けたより現実的な設定における理論的検討，および符号化法の構成は従来手薄となってきた．そこで本研究では，アリスとボブが生成する秘密鍵が一致しない確率の解析や，プロトコル中で用いられる誤り訂正符号の具体的な構成を行う．これにより，従来行われてきた研究の橋渡しすることで，効率的かつ安全な秘密鍵共有プロトコルの実現に寄与することを目的とする．

３．研究の方法

上述の雑音通信路を利用した秘密鍵共有プロトコルのうち，本研究では特に雑音通信路の入力信号列および出力信号列から共通のビット列を生成する手順に注目する．ディジタル通信において標準的なモデルである加法的白色ガウス通信路を雑音通信路として想定し，線形符号を利用する以下のプロトコルを対象とする．

- アリスとボブは，雑音通信路の入出力から信号列の部分列を抽出する．これは信頼性の高い信号から構成され，アリスの送信信号をボブが高い確率で正しく推定できるものを指す．これらの選択は公開通信路を通した交信により行われるため，その内容は第三者も把握可能である．
- アリスは，両者間で予め合意されている線形符号の検査行列を用いて，自らが有する信号列に対するシンドロームを計算し，公開通信路を通してこれをボブに伝達する．
- ボブは，抽出された部分信号列と上記のシンドロームを基に，送信者が持つ信号列を推定する．

本研究では特に受信者が送信者の信号列の推定に失敗する確率に関して理論的検討を行う．上記はスレピアン・ウォルフの符号化と呼ばれる情報理論で知られる手法，すなわち復号器に対して補助的情報が与えられている場合の情報源符号化の問題に相当する．なお，秘密鍵共有プロトコルでは第三者が公開通信路における通信内容を把握可能であることを前提としており，このため通信されるシンドロームが担う情報量を抑制する必要があるため，情報源符号化の問題として定式化される．

線形符号を用いる場合のスレピアン・ウォルフの符号化の性能は，同一の符号を使用した通信路符号化と同等である．その一方，上述の秘密鍵共有プロトコルでは，信頼性の高

い信号列の抽出を行う手順が含まれることから，標準的な解析手法を適用することができない．したがって，この影響を踏まえた誤り確率の理論的解析を信号列の統計的な性質を踏まえて行う必要がある．

また，実用的な観点からは，プロトコルの効率向上のため，スレピアン・ウォルフ符号化に適した性能の高い線形符号を用いる必要があるが，この具体的な構成法についても検討を行う．現在では，確率的反復復号法を適用しうる連接符号が，理論限界に迫る誤り率特性を達成することが示されているが，本研究では反復復号の過程で発生する軟情報の相互情報量を追跡する手法を用いることで，スレピアン・ウォルフ符号化に適した線形符号の具体化を行う．

さらに，より一般的な通信モデルの下で物理層セキュリティを実現することは，学術的にも興味深い課題である．これらには，相関のある連続的な情報源をアリスとボブが共有する場合や，多数の通信ノードが協調的に通信を行う環境などが挙げられる．これらの設定へのプロトコルの拡張を視野に入れ，基本的なツールとなる符号化や量子化の手法に関しても基礎的検討を行う．

４．研究成果

本研究における成果を以下に示す．

(1) 順序つき確率変数列に対するスレピアン・ウォルフ符号化の性能解析

研究方法の欄で述べた通り，秘密鍵共有プロトコルでは，通信路出力から信頼性の高い信号対を抽出し，これに対して誤り訂正を行う．これは順序つき確率変数列に対するスレピアン・ウォルフ符号化として等価的に定式化される．従って，この過程で得られる信号列の統計的性質を踏まえた解析を行う必要がある．本研究では，抽出された信号列に関する結合確率密度を与えた上で，アリスが持つ系列をボブが正しく推定できない事象を考慮することで，誤り確率の上界を導出した．得られた限界式に対して数値計算を行い，計算機シミュレーションによる実験結果と比較することで，タイトな限界式が得られていることを確認した．

また，数値結果より，通常の通信路符号化では見られない以下の現象が発生しうることを観察している： 通信路符号化では，符号語内の記号の配置に対して誤り確率は不変であるが，本研究の設定の下では，誤り確率が記号位置に依存しえる．また，通常の通信路符号化では最小ハミング重みに相当する事象が誤り確率で支配的となるが，本研究の設定の下では最小距離より大きい重みを有する誤り事象が最大の誤り確率を与えることがある．これらは，符号化の対象となっている信号列が順序つき確率変数列となることの直接的な帰結であり，したがって使用される符号の選択は慎重に行われるべきであることを示唆している．以上の成果は，[雑誌論文]③および[学会発表]④で公表している．

一方，以上で得られた誤り確率の上界式は，その数値計算に多重積分を要するため，現実的に評価が行えるのは最小距離が小さい 2 元線形符号に限定される．そこで，より効率的に数値計算を行える近似上界式を導出した．これは，抽出された信号に関する符号のパターンが，発生し得る誤り事象と密接な関連を持つことに着目することで得られた．この近似上界式は厳密な限界式と比して計算量に関して大幅に効率的であるため，最小距離が大きい符号に対しても適用が可能である．その数値計算結果が，計算機シミュレーションや厳密な上界式の数値を正確に予測しえることを[学会発表]②で公表している．

(2) スレピアン･ウォルフ符号化の理論的性能限界に迫る多値線形符号の構成

秘密鍵共有プロトコルを実現する上で，復号性能の高い線形符号を構成することは重要な課題である．ここで，符号が定義される有限体が 2 のべき乗である線形符号は多くの研究成果が示されているが，これ以外の多値線形符号についてはさらなる検討の余地が残されている．本研究では，符号長が比較的短い線形ブロック符号と，符号化率が 1 である畳込み符号を，インタリーバを介して連接した符号を提案した．この符号に対して，確率的反復復号の過程で計算される外部情報と呼ばれる量と，送信記号列との間の相互情報量の変化を追跡することで，計算機シミュレーションの結果と併せて性能評価を行った．これにより，スレピアン・ウォルフ符号化の理論的性能限界に迫る性能が達成されることを[学会発表]⑤にて示している．

(3) 広範な環境におけるプロトコルの実現を目指した基礎検討

物理層セキュリティを実現する上で，通信を行う二者間で相関のある情報源の存在を仮定する場合，情報源出力を離散情報に置き換える量子化の操作を要する．この問題に対して，空間結合と呼ばれる方法論を応用した低密度生成行列符号を用いた場合の量子化法の検討と性能評価を行った．これは，[学会発表]③にて公表している．また，量子化誤差に関して最適性を要する場合には，畳込み符号を用いることが有力である．そこで，量子化の際に用いられるトレリス線図の状態数が大きい畳込み符号に対する性能を計算機実験により評価し，その結果を[雑誌論

文]②で公表している．また，通信ノードが協調的に通信する環境において物理層セキュリティを構築することを視野に，通信路符号化を伴う物理層ネットワーク符号化に関して，誤り確率の理論的解析を[学会発表]①にて行っている．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）

① 井坂 元彦、畳込み符号とターボ符号、映像情報メディア学会誌、査読無、vol. 70、2016、ページ数未定

② Yohei Onishi、Hidaka Kinugasa、Takashi Muraki、Motohiko Isaka、Rate-distortion performance of convolutional codes for binary symmetric source、IEICE Trans. Fundamentals、査読有、vol. 98-A、2015、2480-2482、10.1587/transfun.E98.A.2480

③ Kana Deguchi、Motohiko Isaka、Error performance analysis of asymmetric Slepian-Wolf coding for ordered random variables、IEICE Trans. Fundamentals、査読有、vol. E98-A、2015、992-999、10.1587/transfun.E98.A.992

④ Misako Kotani、Shingo Kawamoto、Motohiko Isaka、Granular gain of low-dimensional lattices from binary linear codes、IEICE Trans. Fundamentals、査読有、vol. E95-A、2012、2168-2170、10.1587/transfun.E95.A.2168

〔学会発表〕（計５件）

① 宗圓 博宜、井坂 元彦、通信路符号化を用いる物理層ネットワーク符号化における性能解析、第 38 回情報理論とその応用シンポジウム、2015 年 12 月 9 日、下電ホテル（岡山県倉敷市）

② Kana Deguchi、Motohiko Isaka、Approximate performance bound for coding in secret key agreement from the Gaussian channel、IEEE Wireless Communications and Networking Conference (WCNC2015)、2015 年 3 月 11 日、New Orleans (USA)

③ 松ヶ下 大輔、井坂 元彦、LDGM 畳込み符号を用いた量子化に関する検討、電子情報通信学会 通信方式研究会、2015 年 2 月 26 日、鳥取大学（鳥取県鳥取市）

④ Kana Deguchi、Motohiko Isaka、Analysis of information reconciliation in secret key agreement from the AWGN channel、IEEE Vehicular Technology Conference (VTC2014-Spring)、2014 年 5 月 20 日、Seoul、Korea

⑤ Motohiko Isaka、Non-binary serially concatenated codes for distributed source coding、International Symposium on Information Theory and its Applications (ISITA2012)、2012 年 10 月 29 日、Honolulu、USA

〔図書〕（計２件）

① Motohiko Isaka (edited by David Declercq, Marc Fossorier, and Ezio Biglieri)、Academic Press、Channel Coding - Theory, Algorithms, and Applications、2014、667 (497-534)

② 楫 勇一、岩田 賢一、葛岡 成晃、井坂 元彦、オーム社、情報・符号理論、2013、200 (121-170)

６．研究組織
(1)研究代表者
井坂 元彦（ ISAKA MOTOHIKO ）
関西学院大学・理工学部・教授
研究者番号： 50351739

(2)研究分担者

なし

(3)連携研究者

なし